Chapitre I

Introduction à la sécurité de l'information

Abdelali Saidi

abdelali.saidi@gmail.com

1. Un overview de la sécurité de l'information
2. Principes de la sécurité de l'information
3. Menaces à la sécurité de l'information
4. Implémentation de la sécurité de l'information

Plan

1. Un overview de la sécurité de l'information
2. Principes de la sécurité de l'information
3. Menaces à la sécurité de l'information
4. Implémentation de la sécurité de l'information

La sécurité des SI

Le système d'information

La sécurité des SI

La sécurité des SI

Le système d'information

Un système d'information est l'ensemble des éléments qui participent à:

La sécurité des SI

La sécurité des SI

Le système d'information

Un système d'information est l'ensemble des éléments qui participent à:

- la gestion de l'information;
- le stockage de l'information;
- le traitement de l'information;
- la diffusion de l'information.

La sécurité des SI

La sécurité des SI

Le système d'information

Un système d'information est l'ensemble des éléments qui participent à:

- la gestion de l'information;
- le stockage de l'information;
- le traitement de l'information;
- la diffusion de l'information.

La sécurité des SI

La sécurité des systèmes d'information réfère à tous les moyens organisationnels, légales, humaines et techniques implémentés pour assurer la sécurité de l'information.

Les niveaux de sécurité

Présentation

Définition pratique

Les niveaux de sécurité

Présentation

- Protections organisationnelles;
- Protections légales;
- Protections humaines;
- Protections techniques.

Définition pratique

Les niveaux de sécurité

Présentation

- Protections organisationnelles;

  La sécurité opérationnelle, La politique de sécurité.
- Protections légales;

  La loi 09-08 sur la protection des personnes à l'égard du traitement des données personnel, La loi 07-03 concerne les systèmes de traitement automatisé des données, La loi 53-05 concerne l'échange de données par voie électronique
- Protections humaines;

  Vérifier les antécédents avant de recruter, Sensibilisation.
- Protections techniques.

  Protections physiques, systèmes, réseaux.

Définition pratique

Les niveaux de sécurité

Présentation

- Protections organisationnelles;

  La sécurité opérationnelle, La politique de sécurité.

- Protections légales;

  La loi 09-08 sur la protection des personnes à l'égard du traitement des données personnel, La loi 07-03 concerne les systèmes de traitement automatisé des données, La loi 53-05 concerne l'échange de données par voie électronique

- Protections humaines;

  Vérifier les antécédents avant de recruter, Sensibilisation.

- Protections techniques.

  Protections physiques, systèmes, réseaux.

Définition pratique

La sécurité de l'information réfère à une protection de tout accès, utilisation, diffusion, modification ou destruction non autorisés.

Plan

1 Un overview de la sécurité de l'information
2 Principes de la sécurité de l'information
3 Menaces à la sécurité de l'information
4 Implémentation de la sécurité de l'information

La triade CIA

Présentation

La sécurité de l'information joue autour de trois principes essentielles (Connus sous le signe CIA):

La triade CIA

Présentation

La sécurité de l'information joue autour de trois principes essentielles (Connus sous le signe CIA):

- la confidentialité (confidentiality);

La triade CIA

Présentation

La sécurité de l'information joue autour de trois principes essentielles (Connus sous le signe CIA):

- la confidentialité (confidentiality);
- l'intégrité (integrity);

La triade CIA

Présentation

La sécurité de l'information joue autour de trois principes essentielles (Connus sous le signe CIA):

- la confidentialité (confidentiality);
- l'intégrité (integrity);
- la disponibilité (availability).

La triade CIA

Présentation

La sécurité de l'information joue autour de trois principes essentielles (Connus sous le signe CIA):

- la confidentialité (confidentiality);
- l'intégrité (integrity);
- la disponibilité (availability).

Tout mécanisme de sécurité existant ou verra le jour sera déployé pour l'amélioration d'au moins l'un de ces principes.

La triade CIA

La confidentialité

Techniques

La triade CIA

La confidentialité

La confidentialité est le fait d'assurer que seules les personnes autorisées ont accès à l'information.

Techniques

La triade CIA

La confidentialité

La confidentialité est le fait d'assurer que seules les personnes autorisées ont accès à l'information.

Techniques

- Le contrôle d'accès;

La triade CIA

La confidentialité

La confidentialité est le fait d'assurer que seules les personnes autorisées ont accès à l'information.

Techniques

- Le contrôle d'accès;
- Le chiffrement de données;

La triade CIA

L'intégrité

Techniques

La triade CIA

L'intégrité

L'intégrité est le fait que l'information ne subisse pas de modification non autorisée, qu'elle soit accidentelle ou bien volontaire.

Techniques

La triade CIA

L'intégrité

L'intégrité est le fait que l'information ne subisse pas de modification non autorisée, qu'elle soit accidentelle ou bien volontaire.

Techniques

- Le contrôle d'accès;

La triade CIA

L'intégrité

L'intégrité est le fait que l'information ne subisse pas de modification non autorisée, qu'elle soit accidentelle ou bien volontaire.

Techniques

- Le contrôle d'accès;
- Le hachage;

La triade CIA

L'intégrité

L'intégrité est le fait que l'information ne subisse pas de modification non autorisée, qu'elle soit accidentelle ou bien volontaire.

Techniques

- Le contrôle d'accès;
- Le hachage;
- Les sauvegardes.

La triade CIA

La disponibilité

Techniques

La triade CIA

La disponibilité

La disponibilité est le fait de garantir qu'un service soit disponible aux utilisateurs légitime.

Techniques

La triade CIA

La disponibilité

La disponibilité est le fait de garantir qu'un service soit disponible aux utilisateurs légitime.

Techniques

- Le contrôle d'accès;

La triade CIA

La disponibilité

La disponibilité est le fait de garantir qu'un service soit disponible aux utilisateurs légitime.

Techniques

- Le contrôle d'accès;
- La redondance;

La triade CIA

La disponibilité

La disponibilité est le fait de garantir qu'un service soit disponible aux utilisateurs légitime.

Techniques

- Le contrôle d'accès;
- La redondance;
- Les sauvegardes.

Principes complémentaires

Définitions

Principes complémentaires

Définitions

- L'authentification: Assurer de l'identité d'une machine distante. Elle est essentielle au déploiement des protocoles de contrôle d'accès.

Principes complémentaires

Définitions

- L'authentification: Assurer de l'identité d'une machine distante. Elle est essentielle au déploiement des protocoles de contrôle d'accès.
- La non répudiation: Assurer qu'aucun des parties prenantes dans une transaction ne puisse renier le fait d'y avoir participer.

Principes complémentaires

Définitions

- L'authentification: Assurer de l'identité d'une machine distante. Elle est essentielle au déploiement des protocoles de contrôle d'accès.
- La non répudiation: Assurer qu'aucun des parties prenantes dans une transaction ne puisse renier le fait d'y avoir participer.
- Anti-rejeu: Assurer la non réutilisation d'une séquence d'un flux enregistré.

Illustration

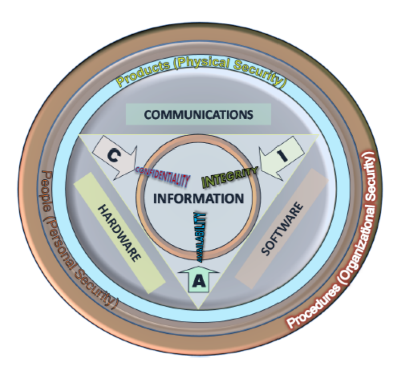


Figure: Confidentiality Integrity Availaibility

Plan

1 Un overview de la sécurité de l'information
2 Principes de la sécurité de l'information
3 Menaces à la sécurité de l'information
4 Implémentation de la sécurité de l'information

Les menaces

Définition

Types de menaces

Les menaces

Définition

Une menace est toute activité qui peut violer un ou plusieurs des principes de la sécurité de l'information. Elle peut parvenir de l'intérieur du système comme elle peut parvenir de l'extérieur.

Types de menaces

Les menaces

Définition

Une menace est toute activité qui peut violer un ou plusieurs des principes de la sécurité de l'information. Elle peut parvenir de l'intérieur du système comme elle peut parvenir de l'extérieur.

Types de menaces

- Menaces liées au personnel;

Les menaces

Définition

Une menace est toute activité qui peut violer un ou plusieurs des principes de la sécurité de l'information. Elle peut parvenir de l'intérieur du système comme elle peut parvenir de l'extérieur.

Types de menaces

- Menaces liées au personnel;
- Menaces liées à l'infrastructure IT;

Les menaces

Définition

Une menace est toute activité qui peut violer un ou plusieurs des principes de la sécurité de l'information. Elle peut parvenir de l'intérieur du système comme elle peut parvenir de l'extérieur.

Types de menaces

- Menaces liées au personnel;
- Menaces liées à l'infrastructure IT;
- Menaces liées au système;

Les menaces

Définition

Une menace est toute activité qui peut violer un ou plusieurs des principes de la sécurité de l'information. Elle peut parvenir de l'intérieur du système comme elle peut parvenir de l'extérieur.

Types de menaces

- Menaces liées au personnel;
- Menaces liées à l'infrastructure IT;
- Menaces liées au système;
- Menaces liées au réseau.

Les menaces

Menaces liées au personnel

Les menaces

Menaces liées au personnel

- Crédulité face au phishing ou à l'ingénierie sociale;

Les menaces

Menaces liées au personnel

- Crédulité face au phishing ou à l'ingénierie sociale;
- Inattention à l'utilisation de disques amovibles;

Les menaces

Menaces liées au personnel

- Crédulité face au phishing ou à l'ingénierie sociale;
- Inattention à l'utilisation de disques amovibles;
- Inattention à l'ouverture de mail;

Les menaces

Menaces liées au personnel

- Crédulité face au phishing ou à l'ingénierie sociale;
- Inattention à l'utilisation de disques amovibles;
- Inattention à l'ouverture de mail;
- Revanche des employés virés.

Les menaces

Menaces liées à l'infrastructure IT

Les menaces

Menaces liées à l'infrastructure IT

- Catastrophes naturelles: tremblement de terre, incendie, inondation;

Les menaces

Menaces liées à l'infrastructure IT

- Catastrophes naturelles: tremblement de terre, incendie, inondation;
- La chambre des serveurs: l'humidité, la température, fuite d'eau;

Les menaces

Menaces liées à l'infrastructure IT

- Catastrophes naturelles: tremblement de terre, incendie, inondation;
- La chambre des serveurs: l'humidité, la température, fuite d'eau;
- Incidents techniques: défaillance du disque dur, sur-chauffage du processeur, coupure ou surcharge d'électricité.

Les menaces

Menaces liées au système

Les menaces

Menaces liées au système

- Erreur de conception de logiciel présentant des failles

Les menaces

Menaces liées au système

- Erreur de conception de logiciel présentant des failles
- Infection de l'environnement

Les menaces

Menaces liées au système

- Erreur de conception de logiciel présentant des failles
- Infection de l'environnement
- Intrusions

Les menaces

Menaces liées au réseau

Les menaces

Menaces liées au réseau

- Erreur de conception de l'architecture pouvant conduire à une congestion et/ou à un déni de service

Les menaces

Menaces liées au réseau

- Erreur de conception de l'architecture pouvant conduire à une congestion et/ou à un déni de service
- Erreur de configuration des noeuds

Les menaces

Menaces liées au réseau

- Erreur de conception de l'architecture pouvant conduire à une congestion et/ou à un déni de service
- Erreur de configuration des noeuds
- Intrusions

Acteurs de l'insécurité informatique



Types de pirates

Acteurs de l'insécurité informatique

Les pirates informatiques

Avant, ce terme désignait les programmeurs surdoués. Aujourd'hui, ce terme réfère à toute personne qui essaye de s'introduire à des systèmes d'information pour différentes raisons.

Types de pirates

Acteurs de l'insécurité informatique

Les pirates informatiques

Avant, ce terme désignait les programmeurs surdoués. Aujourd'hui, ce terme réfère à toute personne qui essaye de s'introduire à des systèmes d'information pour différentes raisons.

Types de pirates

Selon l'éthique du pirate, on peut lui attribuer l'un des noms suivants:

Acteurs de l'insécurité informatique

Les pirates informatiques

Avant, ce terme désignait les programmeurs surdoués. Aujourd'hui, ce terme réfère à toute personne qui essaye de s'introduire à des systèmes d'information pour différentes raisons.

Types de pirates

Selon l'éthique du pirate, on peut lui attribuer l'un des noms suivants:

- white hat : des auditeurs de la sécurité informatique;

Acteurs de l'insécurité informatique

Les pirates informatiques

Avant, ce terme désignait les programmeurs surdoués. Aujourd'hui, ce terme réfère à toute personne qui essaye de s'introduire à des systèmes d'information pour différentes raisons.

Types de pirates

Selon l'éthique du pirate, on peut lui attribuer l'un des noms suivants:

- white hat : des auditeurs de la sécurité informatique;
- black hat : des hors-la-loi expert dans la matière;

Acteurs de l'insécurité informatique

Les pirates informatiques

Avant, ce terme désignait les programmeurs surdoués. Aujourd'hui, ce terme réfère à toute personne qui essaye de s'introduire à des systèmes d'information pour différentes raisons.

Types de pirates

Selon l'éthique du pirate, on peut lui attribuer l'un des noms suivants:

- white hat : des auditeurs de la sécurité informatique;
- black hat : des hors-la-loi expert dans la matière;
- grey hat : des curieux de l'exploit;

Acteurs de l'insécurité informatique

Les pirates informatiques

Avant, ce terme désignait les programmeurs surdoués. Aujourd'hui, ce terme réfère à toute personne qui essaye de s'introduire à des systèmes d'information pour différentes raisons.

Types de pirates

Selon l'éthique du pirate, on peut lui attribuer l'un des noms suivants:

- white hat : des auditeurs de la sécurité informatique;
- black hat : des hors-la-loi expert dans la matière;
- grey hat : des curieux de l'exploit;
- script kiddies : sans grande compétence qui tente tout logiciel disponible;

Acteurs de l'insécurité informatique

Les pirates informatiques

Avant, ce terme désignait les programmeurs surdoués. Aujourd'hui, ce terme réfère à toute personne qui essaye de s'introduire à des systèmes d'information pour différentes raisons.

Types de pirates

Selon l'éthique du pirate, on peut lui attribuer l'un des noms suivants:

- white hat : des auditeurs de la sécurité informatique;
- black hat : des hors-la-loi expert dans la matière;
- grey hat : des curieux de l'exploit;
- script kiddies : sans grande compétence qui tente tout logiciel disponible;
- hacktivistes : ensemble de pirates qui bossent en collaboration afin de répandre un message.

Acteurs de l'insécurité informatique

Les codes malicieux

Les entités

Acteurs de l'insécurité informatique

Les codes malicieux

Une entité contenant un code malicieux essayant de se répandre sans intervention humaine. Elle a généralement comme conséquences: le vole et/ou la destruction de donnée, crashs de systèmes, ...

Les entités

Acteurs de l'insécurité informatique

Les codes malicieux

Une entité contenant un code malicieux essayant de se répandre sans intervention humaine. Elle a généralement comme conséquences: le vole et/ou la destruction de donnée, crashs de systèmes, ...

Les entités

- Virus
- Ver
- Cheval de troie
- Porte dérobée
- L'exploit ...

Acteurs de l'insécurité informatique

Les employés

Exemples de mauvaises utilisations

Acteurs de l'insécurité informatique

Les employés

Les employés de l'entreprise sont la menace la plus dangereuse vu leur acquit d'importants privilèges. Le comportement des employés souvent marche à l'encontre de la politique de sécurité de l'entreprise qu'ils soient conscients ou pas des conséquences de leurs activités personnels.

Exemples de mauvaises utilisations

Acteurs de l'insécurité informatique

Les employés

Les employés de l'entreprise sont la menace la plus dangereuse vu leur acquit d'importants privilèges. Le comportement des employés souvent marche à l'encontre de la politique de sécurité de l'entreprise qu'ils soient conscients ou pas des conséquences de leurs activités personnels.

Exemples de mauvaises utilisations

- Un téléchargement interdit
- Essais d'accès à des emplacements interdits
- Navigation sur des sites web soupçonneux

Plan

1 Un overview de la sécurité de l'information
2 Principes de la sécurité de l'information
3 Menaces à la sécurité de l'information
4 Implémentation de la sécurité de l'information

La roue de la sécurité de l'information

Présentation

La roue de la sécurité de l'information

Présentation

La sécurité de l'information est un processus très dynamique;

La roue de la sécurité de l'information

Présentation

La sécurité de l'information est un processus très dynamique;

L'évolution et l'utilisation native des outils de pénétration impose un processus de sécurité très vigilant et bien aux aguets;

La roue de la sécurité de l'information

Présentation

- La sécurité de l'information est un processus très dynamique;
- L'évolution et l'utilisation native des outils de pénétration impose un processus de sécurité très vigilant et bien aux aguets;
- Tout implémentation de sécurité de l'information doit suivre un processus qu'on appelle la roue de la sécurité;

La roue de la sécurité de l'information

Présentation

- La sécurité de l'information est un processus très dynamique;
- L'évolution et l'utilisation native des outils de pénétration impose un processus de sécurité très vigilant et bien aux aguets;
- Tout implémentation de sécurité de l'information doit suivre un processus qu'on appelle la roue de la sécurité;
- Cette dernière consiste à suivre quatre étapes cyclique pour maximiser le taux de garantie de la sureté de l'information.

La roue de la sécurité de l'information

La roue

La roue de la sécurité de l'information

La roue

Secure: Implémenter des solutions de sécurité;

La roue de la sécurité de l'information

La roue

Secure: Implémenter des solutions de sécurité;

Monitor: Détection d'anomalie;

La roue de la sécurité de l'information

La roue

Secure: Implémenter des solutions de sécurité;

Monitor: Détection d'anomalie;

test: Étude de vulnérabilités et test de pénétration;

La roue de la sécurité de l'information

La roue

Secure: Implémenter des solutions de sécurité;

Monitor: Détection d'anomalie;

test: Étude de vulnérabilités et test de pénétration;

Manage: Analyser les contres-mesures possibles et proposer de nouvelles solutions de sécurité.

La roue de la sécurité de l'information

La roue

Secure: Implémenter des solutions de sécurité;

Monitor: Détection d'anomalie;

test: Étude de vulnérabilités et test de pénétration;

Manage: Analyser les contres-mesures possibles et proposer de nouvelles solutions de sécurité.



Figure: La roue de sécurité

Défense en profondeur

Présentation

Défense en profondeur

Présentation

La sécurité de l'information implique plusieurs domaines (de la sécurité du matériel jusqu'à l'implémentation d'IDS);

Défense en profondeur

Présentation

- La sécurité de l'information implique plusieurs domaines (de la sécurité du matériel jusqu'à l'implémentation d'IDS);
- Une bonne implémentation de sécurité demande un design en plusieurs niveaux;

Défense en profondeur

Présentation

- La sécurité de l'information implique plusieurs domaines (de la sécurité du matériel jusqu'à l'implémentation d'IDS);
- Une bonne implémentation de sécurité demande un design en plusieurs niveaux;
- La défense en profondeur consiste à la sécurisation de chaque niveau

Défense en profondeur

Présentation

La sécurité de l'information implique plusieurs domaines (de la sécurité du matériel jusqu'à l'implémentation d'IDS);

Une bonne implémentation de sécurité demande un design en plusieurs niveaux;

La défense en profondeur consiste à la sécurisation de chaque niveau

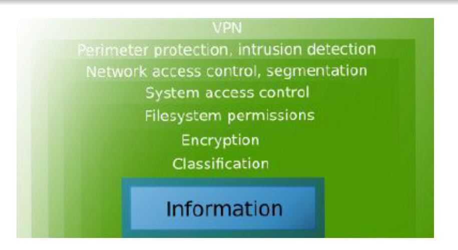


Figure: Information defense in depth